INTERNET PROTOCOL FILTER

Patent number: JP11508753T

Publication date: 1999-07-27

Inventor:

Applicant:

Classification:

- international: H04L12/56; G06F13/00; H04L12/28; H04L12/46; H04L12/66; H04L29/06

- european: H04L12/46B; H04L29/06; H04L29/06C6A; H04L29/12A

Application number: JP19970537534T 19970423

Priority number(s): WO1997CA00269 19970423; US19960015945P 19960424

Also published as:

WO9740610 (A3)
WO9740610 (A2)
EP0895684 (A3)
EP0895684 (A2)
EP0895684 (B1)

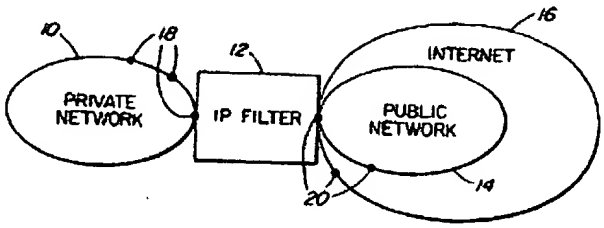
more >>

Report a data error here

Abstract not available for JP11508753T

Abstract of corresponding document: **WO9740610**

The IP filter (12), embodying the present invention, is a communications device designed to provide public network (14) or Internet (16) access to nodes (18) of private networks (10), advantageously without requiring the private nodes on such networks to register public Internet addresses. The IP filter presents a single IP address to the Internet and uses a plurality of IP ports to solve the problem of IP address conservation. It initiates sessions by assigning private side IP sessions to a unique port of the IP filter's public address. The IP filter effects a translation between a source port number for the private network and a destination port number for the public network for communication therebetween. Benefits of the IP filter include private node security and conservation of Internet-registered addresses.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平11－508753

(43)公表日　平成11年(1999)７月27日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ	11/20	１０２Ａ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
Ｈ０４Ｌ	12/28		Ｈ０４Ｌ	11/20	Ｂ
	12/46			13/00	３０５Ｚ
	12/66			11/00	３１０Ｃ

審査請求　有　　予備審査請求　有　（全 41 頁）　最終頁に続く

(21)出願番号　特願平9－537534
(86)(22)出願日　平成９年(1997)４月23日
(85)翻訳文提出日　平成10年(1998)10月22日
(86)国際出願番号　ＰＣＴ／ＣＡ９７／００２６９
(87)国際公開番号　ＷＯ９７／４０６１０
(87)国際公開日　平成９年(1997)10月30日
(31)優先権主張番号　６０／０１５，９４５
(32)優先日　1996年４月24日
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＣＮ，ＪＰ，ＫＲ

(71)出願人　ノーザン・テレコム・リミテッド
カナダ国，エイチ２ワイ　３ワイ４，ケベック，モントリオール，エステイ．アントイン　ストリート　ウェスト　380　ワールド　トレード　センタ　オブ　モントリオール　８フロア
(72)発明者　ウットン・ブルース・アンソニー
アメリカ合衆国，27613，ノースカロライナ州，ラレイ，ベントツイグドライブ　10601
(74)代理人　弁理士　泉　和人

最終頁に続く

(54)【発明の名称】　インターネット・プロトコル・フィルタ

(57)【要約】
本発明のＩＰフィルタ（１２）は、公衆ネットワーク（１４）またはインターネット（１６）アクセスをプライベート・ネットワーク（１０）のノードに提供するために設計された通信デバイスである。ネットワーク上のプライベート・ノードを公衆インターネット・アドレスに登録する必要性がない利点がある。ＩＰフィルタはインターネットに単一のＩＰアドレスを与え、複数のＩＰポートを使ってＩＰアドレス管理の問題を解決している。これはプライベート側のＩＰセッションをＩＰフィルタの公衆アドレスの単一ポートに割り当てることによってセッションを始める。ＩＰフィルタはプライベート・ネットワーク向けのソース・ポート番号と、公衆ネットワーク向けの宛先ポート番号間の翻訳を行う。ＩＰフィルタの利点はプライベート・ノード・セキュリティ、インターネットに登録されたアドレス管理にある。

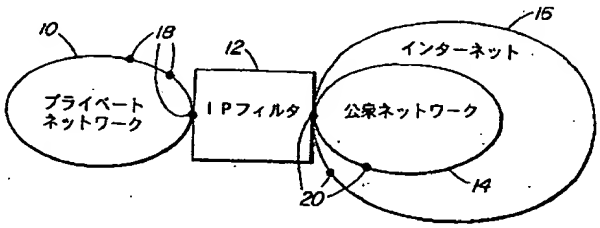


FIG. 1

【特許請求の範囲】

１．　公衆ネットワーク内で知られたアドレスを有するフィルタ・ノードを介してプライベート・データ通信ネットワーク（１０）と公衆データ通信ネットワーク（１４）をインタフェースする方法において：

プライベート・ネットワーク内のノード（１８）からフィルタ・ノードへ宛先情報とソース情報を含んだデータ・パケットをルーティングし、この宛先情報は、公衆ネットワーク内のノード（２０）に対応する宛先アドレスと宛先ポートを含み、そのソース情報は、各プライベート・ネットワーク・ノードのソース・アドレスとソース・ポート含み、

フィルタ・ノードでプライベート・ネットワークから受信された各データ・パケットは、フィルタ・ノードのポートを表わす単一の値と相関関係のあるデータ・パケットから抽出されたソース情報を含み、データ・パケット内でソース・アドレスをフィルタ・ノード・アドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値に置き換え、

公衆ネットワーク内で、各宛先情報に従って、置き換えられたソース情報を含むデータ・パケットをフィルタ・ノードから対応の公衆ネットワーク・ノードにルーティングすることを特徴とする通信ネットワーク・インタフェース方法。

２．　請求項１記載の方法において：

フィルタ・ノードのアドレスを有するデータ・パケット・アドレスを宛先アドレスとして公衆ネットワーク内のノードからフィルタ・ノードにルーティングし、

フィルタ・ノード、公衆ネットワークから受信した各データ・パケットに対して、データ・パケット内の宛先情報の宛先ポートを特定のソース情報に相関させ、データ・パケット内で、宛先情報を特定のソース情報で置き換え、

プライベート・ネットワーク内で、置き換えられた宛先情報を有するデータ・パケットをフィルタ・ノードから対応するプライベート・ネットワーク・ノードにルーティングすることを特徴とする通信ネットワーク・インタフェース方法。

３．　請求項２記載の方法において：

データ・パケット内の宛先情報の宛先ポートが、維持されているソース情報と相関がない場合は、フィルタ・ノードは公衆ネットワークから受信したデータ・パケットを無視することを特徴とする通信ネットワーク・インタフェース方法。

４．　請求項３記載の方法において：

ソース情報を保持するステップは、

各データ・パケットからのソース情報をルックアップ・テーブル中にエントリとしてストアし、ソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブル中にインデックスを構成することを特徴とする通信ネットワーク・インタフェース方法。

５．　請求項４記載の方法において：

データ・パケットはインターネット・プロトコル（ＩＰ）上で送信制御プロトコル（ＴＣＰ）に従ったパケットを含むことを特徴とする通信ネットワーク・インタフェース方法。

６．　請求項５記載の方法において：

フィルタ・ノードで、プライベート・ネットワークからのＴＣＰパケットを受信し、ＴＣＰパケットに対応するエントリがルックアップ・テーブルに見つからず、ＴＣＰパケットが「これは接続リクエストである」と示した場合、ソース情報とＴＣＰパケットからの宛先情報を新しいエントリとしてルックアップ・テーブルにストアすることを特徴とする通信ネットワーク・インタフェース方法。

７．　請求項６記載の方法において：

フィルタ・ノードで、公衆ネットワークからのＴＣＰパケットを受信し、受信されたＴＣＰパケット内のソース・ポートがＴＣＰパケット内の宛先ポートによってインデックスされたルックアップ・テーブルのソース情報エントリ内の宛先ポートと異なり、ＴＣＰパケットが「このパケットは接続リクエストに対する最初の応答である」と示した場合、フィルタ・ノードはテーブル・エントリ内の宛先ポートをＴＣＰパケットから受信されたソース・ポートに更新することを特

徴とする通信ネットワーク・インタフェース方法。

８．　請求項７記載の方法において：

フィルタ・ノードで、パケット内に送信コードの終端を有するＴＣＰパケットを受信し、受信されたＴＣＰパケットに対応するルックアップ・テーブル内のエントリをゼロにすることを特徴とする通信ネットワーク・インタフェース方法。

９．　請求項４記載の方法において：

データ・パケットはインターネット・プロトコル（ＩＰ）上でユーザ・データグラム・プロトコル（ＵＤＰ）に従ったパケットを含むことを特徴とする通信ネットワーク・インタフェース方法。

１０．　請求項９記載の方法において：

フィルタ・ノードで、プライベート・ネットワークからのＵＤＰデータ・パケットを受信し、ルックアップ・テーブル内の新しいエントリとして、ＵＤＰパケットからのソース情報と宛先情報を経過タイマの期間表示と共に追加することを特徴とする通信ネットワーク・インタフェース方法・

１１．　プライベート・データ通信ネットワーク（１０）と公衆データ通信ネットワーク（１４）をフィルタ・ノードを介してインタフェースする方法において：

（ａ）　フィルタ・ノードで、公衆ネットワーク内のノード（２０）に対応した宛先アドレスと、プライベート・ネットワーク内のノード（１８）に対応したソース・アドレスを有するデータ・パケットをプライベート・ネットワークから受信し、

（ｂ）　フィルタ・ノードで、データ・パケットから抽出したソース・アドレスを維持し、

（ｃ）　データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、

（ｄ）　公衆ネットワーク内で、宛先アドレスに従って、置き換えられたソース・アドレスを有するデータ・パケットをフィルタ・ノードから対応する公衆

ネットワーク・ノードにルーティングし、

（ｅ）　置き換えられたソース情報を有するデータ・パケットに応答して公衆ネットワークからの戻りパケットを待ち、

（ｆ）　戻りパケット内で、宛先アドレスを維持されたソース・アドレスと置き換え、

（ｇ）　プライベート・ネットワーク内で、置き換えられた宛先アドレスを有する戻りパケットをフィルタ・ノードから対応するプライベート・ネットワーク・ノードへルーティングすることを特徴とする通信ネットワーク・インタフェース方法。

１２．　請求項１１記載の方法において：

フィルタ・ノードにおいて、戻りパケットを待っている間に、プライベート・ネットワークから受信されたデータ・パケットをさらにバッファリングし、バッファされたパケットがあればそのパケットに対して、ステップ（ｂ）から（ｇ）を繰り返すことを特徴とする通信ネットワーク・インタフェース方法。

１３．　請求項１２記載の方法において：

データ・パケットはインターネット制御メッセージ・プロトコル（ＩＣＭＰ）に従ったパケットを含むことを特徴とする通信ネットワーク・インタフェース方法。

１４．　第１のデータ通信ネットワーク（１０）および第２のデータ通信ネットワーク（１４）をインタフェースするフィルタ・ノード（１２）を動作させる方法において：

宛先情報とソース情報を有するデータパケットを第１のネットワークから受信し、その宛先情報は、第２のネットワーク内のノード（２０）に対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第１のネットワーク内のノード（１８）に対応するソース・アドレスとソース・ポートを有し、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに

置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、

置き換えられたソース情報を有するデータ・パケットを第２のネットワークに送り、それによってそのパケットは宛先情報に従って対応する第２のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

１５．　請求項１４記載の方法において：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第２のネットワークから受信し、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させ、

データ・パケット内で、宛先情報を特定のソース情報と置き換え、

置き換えられた宛先情報を有するデータ・パケットを第１のネットワークに送り、それによってそのパケットが宛先情報に従って対応の第１のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

１６．　請求項１５記載の方法において：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第２のネットワークから受信されたデータ・パケットを無視することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

１７．　請求項１６記載の方法において：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアし、ソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

１８．　請求項１７記載の方法において：

データ・パケットはインターネット・プロトコル（ＩＰ）上で送信制御プロ

トコル（ＴＣＰ）に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

１９．　請求項１８記載の方法において：

第１のネットワークからＴＣＰパケットを受信し、そのＴＣＰパケットに対応するエントリがルックアップ・テーブルに見つからず、そのＴＣＰパケットが「これは接続リクエストである」と示した場合、ソース情報をＴＣＰパケットからの宛先情報と共に、ルックアップ・テーブル内の新しいエントリとしてストアすることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２０．　請求項１９記載の方法において：

第２のネットワークからＴＣＰパケットを受信し、受信されたＴＣＰパケット内のソース・ポートが、ＴＣＰパケット内の宛先ポートによってインデックスされたルックアップ・テーブルのソース情報エントリ内の宛先ポートと異なり、またＴＣＰパケットが「このパケットが接続リクエストに対する最初の応答である」ことを示した場合には、テーブル・エントリ内の宛先ポートを受信したＴＣＰパケットからのソース・ポートで更新することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２１．　請求項２０記載の方法において：

パケット内の送信コードの終端を有するＴＣＰパケットを受信し、受信されたＴＣＰパケットに対応するルックアップ・テーブル内のエントリをゼロにすることことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２２．　請求項１７記載の方法において：

データ・パケットはインターネット・プロトコル（ＩＰ）上でデータグラム・プロトコル（ＵＤＰ）に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２３．　請求項２２記載の方法において：

第１のネットワークからのＵＤＰデータ・パケットを受信し、ルックアップ

・テーブル内の新しいエントリとして、ＵＤＰパケットからのソース情報と宛先情報を経過タイマの期間表示と共に追加することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２４．　第１のデータ通信ネットワーク（１０）と第２のデータ通信ネットワーク（１４）をインタフェースするフィルタ・ノード（１４）を動作させる方法において：

（ａ）　第２のネットワーク内のノード（２０）に対応する宛先アドレスと第１のネットワーク中のノード（１８）に対応するソース・アドレスとを有するデータ・パケットを第１のネットワークから受信し、

（ｂ）　データ・パケットから抽出されたソース・アドレスを維持し、

（ｃ）　データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、

（ｄ）　置き換えられたソース・アドレスを有するデータ・パケットを第２のネットワークに送り、それによってそのパケットは対応の第２のネットワーク・ノードにルーティングされ、

（ｅ）　置き換えられたソース情報を有するデータ・パケットに応じて、第２のネットワークからの戻りパケットを受信し、

（ｆ）　戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換え、

（ｇ）　置き換えられた宛先アドレスを有する戻りパケットを第１のネットワークに送り、それによってそのパケットは対応の第１のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２５．　請求項２４記載の方法において：

戻りパケットを待つ間に第１のネットワークから受信されたータ・パケットをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ（ｂ）から（ｇ）を繰り返すことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２６．　請求項２５記載の方法において：

データ・パケットはインターネット制御メッセージ・プロトコル（ＩＣＭＰ）に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

２７．　第１のデータ通信ネットワーク（１０）と第２のデータ通信ネットワーク（１４）をインタフェースするフィルタ・ノード（１２）において：

第２のネットワーク内のノード（２０）に対応する宛先アドレスと宛先ポートを有する宛先情報と、第１のネットワーク内のノード（１８）に対応するソース・アドレスとソース・ポートを有するソース情報とを有するデータパケットを第１のネットワークから受信する手段と、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持する手段と、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換える手段と、

置き換えられたソース情報を有するデータ・パケットを第２のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第２のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

２８．　請求項２７記載のフィルタ・ノードにおいて：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第２のネットワークから受信する手段と、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させる手段と、

データ・パケット内で、宛先情報を特定のソース情報と置き換える手段と、

置き換えられた宛先情報を有するデータ・パケットを第１のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第１のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

２９．　請求項２８記載のフィルタ・ノードにおいて：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第２のネットワークから受信されたデータ・パケットを無視する手段を備えたことを特徴とするフィルタ・ノード。

３０．　請求項２９記載のフィルタ・ノードにおいて：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアする手段を備え、そのソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成することを特徴とするフィルタ・ノード。

３１．　第１のデータ通信ネットワーク（１０）と第２のデータ通信ネットワーク（１４）をインタフェースするフィルタ・ノード（１２）において：

（ａ）　第２のネットワーク内のノード（２０）に対応する宛先アドレスと第１のネットワーク中のノード（１８）に対応するソース・アドレスとを有するデータ・パケットを第１のネットワークから受信する手段と、

（ｂ）　データ・パケットから抽出されたソース・アドレスを維持する手段と、

（ｃ）　データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換える手段と、

（ｄ）　置き換えられたソース・アドレスを有するデータ・パケットを第２のネットワークに送り、それによってそのパケットを対応の第２のネットワーク・ノードにルーティングする手段と、

（ｅ）　置き換えられたソース情報を有するデータ・パケットに応じて、第２のネットワークからの戻りパケットを受信する手段と、

（ｆ）　戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換える手段と、

（ｇ）　置き換えられた宛先アドレスを有する戻りパケットを第１のネットワークに送り、それによってそのパケットを対応の第１のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

３２．　請求項３１記載のフィルタ・ノードにおいて：

戻りパケットを待つ間に第１のネットワークから受信されたデータ・パケットをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ（ｂ）から（ｇ）を繰り返す手段を備えたことを特徴とするフィルタ・ノード。

【発明の詳細な説明】

発明の名称

インターネット・プロトコル・フィルタ

発明の分野

本発明は一般的に、インターネット・ファイアウォールに関する。特に、プライベート・インターネット・プロトコル（ＩＰ）ネットワーク・ドメインを公衆インターネット上の単一ＩＰアドレスにマッピングするインターネット・プロトコル・フィルタに関する。

背景技術

ファイアウォールは、一般的に、プライベート・ネットワークのドメイン内のノードをインターネットのような公衆ネットワーク内のノードに結びつける機能を有するコンピュータサーバとして知られ、特徴づけられる。公知のファイアウォール製品の欠点として、セッションの同時発生または公衆ノードとプライベート・ノード間の相互作用に対して、独自の公衆ＩＰアドレスが必要になることが知られている。このため、公衆ＩＰアドレスを管理するファイアウォールが望まれていた。

発明の概要

本発明の目的は、２つのネットワーク間の通信を結合する新しい改良された装置を提供することにある。

本発明の第１の側面によると、本発明は、公衆ネットワーク内で知られたアドレスを有するフィルタ・ノードを介してプライベート・データ通信ネットワークと公衆データ通信ネットワークをインタフェースする方法において：プライベート・ネットワーク内のノードからフィルタ・ノードへ宛先情報とソース情報を含んだデータ・パケットをルーティングし、この宛先情報は、公衆ネットワーク内のノードに対応する宛先アドレスと宛先ポートを含み、そのソース情報は、各プライベート・ネットワーク・ノードのソース・アドレスとソース・ポート含み、フィルタ・ノードでプライベート・ネットワークから受信された各データ・パケットは、フィルタ・ノードのポートを表わす単一の値と相関関係のあるデータ・

パケットから抽出されたソース情報を含み、データ・パケット内でソース・アドレスをフィルタ・ノード・アドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値に置き換え、公衆ネットワーク内で、各宛先情報に従って、置き換えられたソース情報を含むデータ・パケットをフィルタ・ノードから対応の公衆ネットワーク・ノードにルーティングするように構成される。

本発明の第２の側面によれば、本発明は、プライベート・データ通信ネットワークと公衆データ通信ネットフークをフィルタ・ノードを介してインタフェースする方法において：（ａ）フィルタ・ノードで、公衆ネットワーク内のノードに対応した宛先アドレスと、プライベート・ネットワーク内のノードに対応したソース・アドレスを有するデータ・パケットをプライベート・ネットワークから受信し、（ｂ）フィルタ・ノードで、データ・パケットから抽出したソース・アドレスを維持し、（ｃ）データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、（ｄ）公衆ネットワーク内で、宛先アドレスに従って、置き換えられたソース・アドレスを有するデータ・パケットをフィルタ・ノードから対応する公衆ネットワーク・ノードにルーティングし、（ｅ）置き換えられたソース情報を有するデータ・パケットに応答して公衆ネットワークからの戻りパケットを待ち、（ｆ）戻りパケット内で、宛先アドレスを維持されたソース・アドレスと置き換え、（ｇ）プライベート・ネットワーク内で、置き換えられた宛先アドレスを有する戻りパケットをフィルタ・ノードから対応するプライベート・ネットワーク・ノードへルーティングするように構成される。

本発明の第３の側面によれば、本発明は、第１のデータ通信ネットワークおよび第２のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：宛先情報とソース情報を有するデータパケットを第１のネットワークから受信し、その宛先情報は、第２のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第１のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有し、フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、データ・パケット内で、ソース・アドレスをフィルタ・

ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、置き換えられたソース情報を有するデータ・パケットを第２のネットワークに送り、それによってそのパケットは宛先情報に従って対応する第２のネットワーク・ノードにルーティングされるように構成される。

本発明の第４の側面によれば、本発明は、第１と第２のデータ通信をインタフェースするフィルタ・ノードを提供する。このフィルタ・ノードは、フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第２のネットワークから受信する手段と、データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させる手段と、データ・パケット内で、宛先情報を特定のソース情報と置き換える手段と、置き換えられた宛先情報を有するデータ・パケットを第１のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第１のネットワーク・ノードにルーティングする手段とを備えるように構成される。

本発明で実現されるＩＰフィルタは、公衆ネットワークやインターネット・アクセスをプライベート・ネットワークのノードに供給するために設計された通信デバイスである。ＩＰフィルタは、ネットワーク上でプライベート・ノードを必要とせず、公衆インターネット・アドレスに登録できることを利点とする。ＩＰフィルタはインターネットに単一ＩＰアドレスを与え、複数のＩＰポートを使ってＩＰアドレス管理の問題を解決する。ＩＰフィルタはプライベート側のＩＰセッションをＩＰフィルタの公衆アドレスの単一ポートに割り当てることによってセッションを開始する。これによって最大で64,512（65,536-1,024 ポート）の同時セッションが単一ＩＰアドレスでサポートされる。ＩＰフィルタはプライベート・ネットワーク用のソース・ポート番号と、公衆ネットワーク用の宛先ポート番号間で通信を行うための翻訳を行う。ＩＰフィルタはプライベート・ノードのセキュリティ、インターネットに登録されたアドレス管理などに利点がある。

特定の実施の形態として、ＩＰフィルタはインターネット・プロトコル上で３つのデータ伝送プロトコルをサポートできる。送信コントロールプロトコル（ＴＣＰ）、ユーザ・データグラム・プロトコル（ＵＤＰ）、およびインターネット

制御メッセージ・プロトコル（ＩＣＭＰ）の３つである。他のプロトコルのパケットは無視される。

ＴＣＰプロトコルはＴＣＰヘッダをデータ・パケットに付加する。ソース・ポートと宛先ポートの番号はこのヘッダ内に含まれる。ソース・ノードと宛先ノードのインターネット・アドレスはＩＰヘッダ内に含まれる。各パケットから抽出されたＩＰアドレスとポート情報を使って、ＩＰフィルタはこのパケットをどこにルーティングするかを決定する。

ＩＰフィルタは各ＴＣＰ接続上で情報のルックアップ・テーブルを保持する。この情報にはプライベート・ノードからのポート、プライベートＩＰアドレス、宛先ノードの割り当てポート番号、ＩＰフィルタのポート番号をインデックスの形で含んでいる。パケットをプライベート・ネットワークから受け取ると、このパケットに対応するエントリがテーブル中に見つからず、ＴＣＰヘッダが「これは新しい接続リクエストである」ことを示した場合、プライベート・アドレスとポート番号は新しいエントリとしてテーブルに追加される。その後、パケット・ヘッダ内のソース・アドレスとポート番号はＩＰフィルタのＩＰアドレスとポート番号に置き換えられ、パケットはインターネットに送信される。

ＩＰフィルタは、インターネットからパケットを受け取ると、宛先ポート番号を使ってルックアップ・テーブルにインデックスを付ける。対応のテーブル・エントリが見つかると、宛先アドレスとポート番号はプライベート・ネットワークのＩＰアドレスとポート番号に置き換えられ、パケットはプライベート・ネットワークに送信される。受け取ったパケットのソース・ポートがテーブルに記録されたポートと異なる場合、またパケット・ヘッダ情報が「このパケットは接続上で最初の応答である」ことを示した場合、ルックアップ・テーブルは必要に応じてインターネット・ノードによって割り当てられたポート番号で更新される。

ＩＰフィルタがパケット内で送信コードの終わりを検出すると、ルックアップ・テーブル・エントリは０にリセットされる。ＩＰフィルタがＩＰフィルタ・ポートに対応するルックアップ・テーブルの中にエントリを持たないインターネットからパケットを受け取ると、ＩＰフィルタはそのパケットを無視する。

ＵＤＰプロトコルはＴＣＰとは逆に、接続レス、または接続指向プロトコルである。ＵＤＰヘッダは初期接続または送信終了を制御するコードを含まない。ＵＤＰヘッダ内で関係のあるデータはソース・ポートと宛先ポートである。この情報はＩＰヘッダに含まれたインターネット情報を共に使用され、ＩＰフィルタがどこにパケットをルーティングするかを決める。

ＩＰフィルタは各ＵＤＰセッション上で情報のルックアップ・テーブルを保持する。ＩＰフィルタがプライベート・ネットワークからＵＤＰパケットを受け取ると、ＩＰフィルタはソース・アドレス、ソース・ポート番号、宛先ポート番号、および割り当てられたＩＰフィルタ・ポート番号をテーブルのインデックスとして記録する。次にパケット・ヘッダ内のプライベート・ノード・アドレスとポート番号は、ＩＰフィルタのアドレスと割り当てポート番号に置き換えられる。その後、パケットはインターネットに送信される。

ＩＰフィルタがインターネットからＵＤＰパケットを受け取ると、ＩＰフィルタはＵＤＰルックアップ・テーブルにインデックスをつけ、パケットの宛先情報つまりＩＰフィルタ・アドレスと割り当てポート番号を、ルックアップ・テーブルからのプライベート・アドレスとポート番号に置き換える。ルックアップ・テーブルは、また、標準ＵＤＰの実行によって受け取ったデータグラム・パケット

上の経過タイマの期間表示を保持する。ＩＰフィルタがＩＰフィルタ・ポートに対応するルックアップ・テーブルの中でエントリを持たないインターネットからのパケットを受け取ると、フィルタはそのパケットを無視する。

ＩＣＭＰパケットはソース・ポート番号も宛先ポート番号も持っていないので、プライベート・ネットワークから受け取ったＩＣＭＰパケットは１度に１つだけ、追加ＩＣＭＰパケットのバッファリングで処理される。ＩＰフィルタはパケット・ヘッダからプライベート・アドレスを読み、それをＩＰフィルタのアドレスと置き換える。パケットはインターネットに送信され、ＩＰフィルタは応答を待つ。ＩＰフィルタが応答パケットを受け取ると、パケット・ヘッダ内の宛先アドレスはＩＰフィルタの宛先アドレスからプライベート・ネットワーク上のノードの宛先アドレスに変わる。次にＩＰフィルタはこのパケットをプライベート・

ネットワークに送信する。

ＩＰプロトコル上でパケットを問題なく送信するためには、各ノードは他のホストのＩＰアドレスとイーサネットベースのデータ通信ネットワーク内のそれに対応するイーサネット・アドレスのテーブルを保持していなければならない。ノードは実際にはＩＰアドレスとイーサネット・アドレスを使ってパケットをアドレスする。この２つのアドレスの関係はダイナミックであり、すなわち、ＩＰアドレスを有するノードはイーサネット・アドレスを変えることができる。アドレス・テーブル内の情報は、ＡＲＰパケットのノードの放送に対する応答から得られる。ソース・ノードはＡＲＰパケットを放送し、宛先ノードのＩＰが与えられると、宛先ノードのイーサネット・アドレスをリクエストする。宛先ノードがパケットを受け取ると、その宛先ノードはリクエストされた情報を有する応答パケットを送る。

ＩＰフィルタは、真のＡＲＰテーブルを保持していないが、ＴＣＰとＵＤＰのパケット通過と同じ方法で、ＡＲＰパケットを送る。ＩＰフィルタが公衆ネットワークの宛先を有するプライベート・ネットワーク上のノードからＡＲＰパケットを受け取ると、ソース・アドレス情報をフィルタのアドレス情報に置き換える。プライベート・ノードのＩＰアドレスとターゲットＩＰアドレスはルックアップ・テーブルの中に入れられる。ターゲット・ノードがそれ自身のイーサネット・アドレスで応答すると、宛先アドレス情報はＩＰフィルタの情報からプライベート・ノードの情報に変わり、その後パケットがプライベート・ノードに送信される。プライベート・ノード・アドレス情報はテーブルから得られる。ＡＲＰパケットがファイアウォールに向けられていると、ＡＲＰパケットはＩＰフィルタを通らず、フィルタと相手のネットワークの間で通信が遮断される。

ＩＰフィルタによって生じるイベントやエラーはログとして登録され、たとえば、テキスト・ファイルの中に記録される。

理想的には、ＩＰフィルタはネットワークからパケットを受け取ってすぐに処理するのが望ましいが、ネットワーク通信が過負荷の場合、ＩＰフィルタはパケットをプライベート・ネットワーク用とインターネット用の２つの待ち行列の中

にバッファリングする。

２つのソース・ルックアップ・テーブルと宛先ルックアップ・テーブルを、前者はＴＣＰパケット用、後者はＵＤＰパケット用に使用してもよい。各テーブルは、通信セッションに割り当てられたＩＰフィルタ・ポート番号によって直接インデックスされる。テーブルのエントリはプライベート・ノードのＩＰアドレス、プライベート・ノードのソース・ポート、およびインターネット・ノードの宛先ポートを含む。特定のＩＰフィルタ・ポートに接続がない場合、テーブル中の対応のエントリは０にリセットされる。プライベート・ネットワークとインターネットの両方から到着したパケットは同じルックアップ・テーブルを使って処理される。この構成では、使用可能なＩＰフィルタ通信ポートの中でパケットのいくつかの宛先がＵＤＰに、いくつかの宛先がＴＣＰに指定されていると仮定している。

図面の簡単な説明

本発明は、添付の図面および次の説明から理解される。

図１はプライベート・ネットワークと公衆ネットワークを結合する１つのインターネット・プロトコルフィルタを表す概略図である。

図２はフィルタ内部のコンポーネントを表わすブロック図である。

発明の実施の形態

図１は、インターネット・プロトコル（ＩＰ）フィルタ１２を通じて公衆ネットワーク１４に接続されるプライベート・ネットワーク１０を示す図である。この公衆ネットワーク１４はインターネット１６とも呼ばれるグローバル・データ・ネットワークの一部を形成する。プライベート・ネットワーク１０は、ローカルエリア・ネットワーク（ＬＡＮ）のような既存のデータ通信ネットワークを表し、プライベート・ネットワークのドメイン内で単一のＩＰアドレスによって識別される複数のノード１８を有する。公衆ネットワーク１４とインターネット１６は公衆ドメインデータ通信ネットワークを表し、それぞれ対応するＩＰアドレスを有する複数のノード２０を有する。

ＩＰフィルタ１２はゲートウェイとして機能し、そこを通してデータ・パケッ

トがプライベート・ネットワーク１０と公衆ネットワーク１４間で交換され、それによってプライベート・ネットワーク１０のノード１８にインターネット・アクセスを行う。ＩＰフィルタ１２はプライベート・ネットワーク・ノード１８の１つを構成し、インターネットに登録された公衆ＩＰアドレスを有する唯一のノードである。これによってＩＰフィルタ１２は本質的に公衆ノード２０の１つをも構成し、そのＩＰアドレスは公衆ドメイン内で知られる。他のプライベート・ネットワーク・ノード１８のＩＰアドレスはプライベート・ネットワーク１０に対して保存され、公衆インターネット・アドレス・ドメイン内では知られず、登録もされない。従来と同様、ＩＰフィルタ１２の関連ＩＰアドレスは複数のＩＰポートであり、全部で65,536あり、そのうち特に64,512は既定のプロトコル用に保存されず、アドレスの翻訳のために使うことができる。

プライベート・ネットワーク１０上のノード１８間の通信は、ＩＰフィルタ１２の存在によって影響を受けることはないが、公衆ネットワーク１４、特にその中のノード２０にアクセスするために、プライベート・ノード１８はすべての通信リクエストを、ＩＰフィルタ１２を通してルーティングする。ＩＰフィルタ１２は、プライベート・ノード１８とインターネット・ノード２０間の通信を、プライベート・ネットワーク１０から受け取ったデータ・パケットのヘッダ情報を修正することによって管理し、その後各通信を公衆ネットワーク１４に送信する。この修正によりプライベート・ノード１８と公衆インターネット・ノード２０間の通信は、実際にはＩＰフィルタ１２とインターネット・ノード２０間の通信になり、すべての戻り通信をＩＰフィルタ１２にルーティングし、次に、戻りデータ・パケットをプライベート・ノード１８にルーティングする。

ＩＰフィルタ１２は、公衆ネットワーク１４からは接続リクエストを受け取らない。プライベート・ノード１８と公衆ノード２０間の通信はすべて、プライベート・ノード１８によって始められる。ＩＰフィルタ１２はインターネット・プロトコル上でＴＣＰ、ＵＤＰおよびＩＣＭＰメッセージの３つのデータ伝送プロトコルをサポートするように設計されており、他のプロトコルのパケットは拒否されるか無視される。

翻訳テーブルはＩＰフィルタ１２によって保持され、プライベート・ネットワーク１０から受信した公衆ネットワーク１４向けのパケットに対するアドレスとポートをマッピングする。翻訳テーブルは各エントリに対して以下の項目を含む。

プライベートＩＰアドレス　　（ｐＩＰ）

プライベートポート　　（ｐＰｏｒｔ）

インターネット（公衆）ＩＰアドレス　　（ｉＩＰ）

インターネット（公衆）ポート　　（ｉＰｏｒｔ）

タイマ

セッションのタイプ／状態

イーサネット・アドレス

基本的な翻訳は、プライベート・ネットワーク側からのＩＰアドレスとポートをＩＰフィルタのＩＰアドレスとポートに置き換え、これによってプライベート・ネットワーク１０上のすべてのノードを公衆ネットワーク１４から隠す。

プライベート・ネットワーク側からのパケットは、ソースと宛先（ｐＩＰ、ｐＰｏｒｔ　－　ｉＩＰ、ｉＰｏｒｔ）を指定する。

これは「ソケット」を定義し、その中で接続の両端（ソースと宛先）はＩＰヘッダ内のＩＰアドレスとＴＣＰまたはＵＤＰヘッダ内のポートによって定義される。

ＩＰフィルタ１２は上記を（ｆｒＩＰ、ｆｒＰｏｒｔ　－　ｉＩＰ、ｉＰｏｒｔ）のように翻訳する。

ここでｆｒＩＰは公衆ネットワーク１４上のＩＰフィルタ１２のＩＰアドレスであり、ｆｒＰｏｒｔは翻訳テーブル＋オフセット値へのインデックスである。このオフセット値は、たとえば、1024であり、よく知られたポートを使ってスキップする。ｆｒＰｏｒｔは任意のポートを表わす。

インターネット・ノード２０は次のパケットで返答する。

（ｉＩＰ、ｉＰｏｒｔ　－　ｆｒＩＰ、ｆｒＰｏｒｔ）

これをＩＰフィルタ１２が受け取り、次のように翻訳する。

（ｉＩＰ、ｉＰｏｒｔ　－　ｐＩＰ、ｐＰｏｒｔ）

一般的にプライベート側から翻訳するには、（プロトコルタイプ、ｐＩＰ、ｐＰｏｒｔ、ｉＩＰ、ｉＰｏｒｔ）の値は翻訳テーブルの中になければならない。これはハッシュ・テーブルを参照して行う必要がある。

公衆側からの翻訳は、直接テーブルを表をして行うことができる。ｆｒＰｏｒｔ－１０２４はテーブルへのインデックスであるからである。パケット内の（ｉＩＰ、ｉＰｏｒｔ）がテーブル中の対応するエントリにマッチしていない場合、承認されていないアクセスは登録され、パケットは捨てられる。

翻訳パケット内でポートがＴＣＰまたはＵＤＰヘッダ内で置き換えられると、ＴＣＰ／ＵＣＰとＩＰヘッダ内のチェックサムを再計算しなければならない。ＩＰアドレスがＩＰヘッダの中で置き換えられると、ＩＰヘッダチェックサムを再計算しなければならない。

以下はＩＰフィルタ１２がサポートする異なるプロトコルについて、特に注意すべき点である。

ＴＣＰの場合、ＳＹＮパケットをプライベート・ネットワーク１０から受け取ると、ＩＰフィルタ１２は使われていないエントリをテーブル中に入れ、その中を埋め、タイプをＴＣＰに、状態をＳＹＮに設定する。その後パケットは上記の一般的な構成によって送られる。テーブル中に空のエントリがないとパケットは捨てられ、イベントが登録される。

ＳＹＮパケットを公衆ネットワーク１４インタフェースから受け取ると、それは、認可されないものとして扱われ、登録される（但し、以下のようなＦＴＰの特別のケースは除く）。しかし、翻訳テーブル・エントリの状態がＳＹＮの場合にはＳＹＮ＋ＡＣＫパケットが送られる。このようなパケットを送った後、状態はＯＰＥＮに設定される。

ＩＰフィルタがＦＩＮパケットを受け取り、翻訳テーブル内の状態がＦＩＮでなかった場合、その状態はＦＩＮに設定され、そのパケットは送られる。状態がＦＩＮの場合、パケットは送られ翻訳テーブル・エントリは０に設定することによって削除される。ＦＩＮはそれぞれの側に送られ、ＴＣＰ接続は終了する。Ｒ

ＳＴパケットを受け取ると、翻訳テーブル・エントリは削除される。

ＵＤＰプロトコルに関し、いずれかのＵＤＰパケットをプライベート・ネットワーク１０側から受け取ると、ＩＰフィルタ１２は、まず標準的な参照を試みる。翻訳テーブル・エントリが見つからない場合には、使われないエントリが設定され、状態はＯＰＥＮに設定される。空のエントリがブランク中に見つからない場合には、パケットを捨てる代わりにテーブル中のランダムＵＤＰが上書きされる。ＵＤＰは非接続で信頼できない送信であるので、エントリの上書きが必要であったパケットを公衆ネットワーク１４から受け取ると、そのパケットは捨てられ、プライベート側上のノード１８は再度試みを行う。

ＦＴＰに関し、ＦＴＰクライアントは、ポート２１などの特定のポート上のＦＴＰサーバとＴＣＰ「制御」接続を確立する。しかしながら、データを送信する必要がある場合、ＦＴＰサーバは、たとえば、デフォルトでは２０になっている「データ」ポートからのＴＣＰ接続を、クライアントが指定した宛先ポートにオープンにする。

これをサポートするために、プライベート・ネットワーク１０からポート２０に送られたパケットは、ＩＰフィルタ１２でＦＴＰ「ポート」コマンドに対して分析される必要がある。検出された場合、テーブル中の新しいエントリを、ｐＰｏｒｔを用いて、ＦＴＰポート・コマンド内の値に設定しなければならない。ＦＴＰコマンド内のＩＰアドレスとポート番号は、パケットを送る前に、ＩＰフィルタのアドレスとポートに変換しなければならない。状態はＦＴＰＤＡＴＡに設定される。

ＳＹＮパケットを公衆ネットワーク１４から受け取り、テーブル・エントリが存在してＦＴＰＤＡＴＡ状態にある場合、パケットは送られ、状態はＯＰＥＮに設定される。

ＩＣＭＰプロトコルに関し、ＩＣＭＰパケットをプライベート・ネットワーク１０から受け取ると、そのパケットがエコー・リクエスト（ピング）の場合、ＩＰフィルタ１２は、新しいエントリを翻訳テーブルの中に置く。パケットのシー

ケンス・フィールドはテーブル中のｐＰｏｒｔに保存され、テーブル・インデックスはパケットのシーケンス・フィールド内に置かれる。ＩＣＭＰチェックサムは再計算され、標準ＩＰヘッダの置換が行われる。このタイプはＩＣＭＰ、状態はＰＩＮＧに設定され、タイマは１分に設定される。

エコー応答（ピング）を公衆ネットワーク１４のインタフェースから受け取ると、シーケンス・フィールドはテーブルへのインデックスとして使われる。状態がＰＩＮＧの場合、テーブル中のｐＰｏｒｔはパケットのシーケンス・フィールドに置き換えられ、ＩＣＭＰチェックサムが再計算され、標準ＩＰヘッダの置き換えが行われる。その後、テーブル・エントリは削除される。

エコー・リクエスト（ピング）を公衆ネットフーク１４から受信すると、ＩＰフィルタ１２が応答する。これによってインターネット・アクセスが可能になりＩＰフィルタ１２に到達し、ＩＰフィルタ１２が実行されていることが確認できる。

宛先に到達できなかったパケットを公衆ネットワーク１４から受け取ると、含まれているヘッダ情報が抽出される。プロトコルがＴＣＰまたはＵＤＰであった場合、送信側のパケットの（ｆｒＩＰ、ｆｒＰｏｒｔ　－　ｉＩＰ、ｉＰｏｒｔ）が決定され翻訳テーブル・エントリの位置が決められる。ＩＣＭＰから抽出されたＩＰアドレスが、テーブル中のアドレスにマッチしていた場合、ＩＰフィルタ１２は、標準の構成を使ってパケットをプライベート・ネットワーク１０に送る。その他のＩＣＭＰパケットは、どちらの側から送られたものでも捨てられ、登録される。

ほとんどのデータ通信プロトコルはＵＤＰプロトコルまたはＴＣＰプロトコルに基づいているので、クライアントへの戻り接続をサーバにオープンさせるＦＴＰのように交渉を始めない限り、これらの他のプロトコルはＩＰフィルタ１２と

互換性がある。他に互換性のあるプロトコルは、Ｔｅｌｎｅｔ、ＴＦＴＰ（小さなファイル送信プロトコル）、ＤＮＳ（ドメイン名サービス）、およびウェブブラウザなどである。

パケットはどちらの方向に送られても、翻訳テーブル・エントリ内のタイマ・

フィールドは計算タイムアウト値（ピングを除く）に設定される。テーブル中にあるすべてのアクティブ・エントリのタイマ・フィールドは１分きざみで減少し、０になると、翻訳テーブル・エントリは削除される。これによって、もはや使われていないＵＤＰエントリとＰＩＮＧエントリ、また、不正に終了してＦＩＮをどちらの側にも送っていないＴＣＰエントリが消去される。使われていないエントリをテーブル中に長く置いておくと安全上問題になる可能性がある。適切な計算タイムアウト値は、典型的なＴＣＰの時間より少しだけ長いものである。

特定の実施の形態では、プライベート・ネットワーク１０と公衆ネットワーク１４はイーサネットベースのＬＡＮである。ＩＰフィルタ１２は、データ処理プラットフォームによって実行され、このプラットフォームはそれぞれネットワーク１０と１４に接続された２つの既存のイーサネット・ハードウェア・インタフェースを備えており、適当なソフトウェアを備え、ＩＰフィルタ１２の機能を実行する。

図２は、データ処理プラットフォームによって実行できるソフトウェアという点から見たＩＰフィルタ１２の内部コンポーネントを示す図である。内部コンポーネントは２つのパケットドライバ３０と３２、アドレス解像プロトコル（ＡＲＰ）テーブル３４、イーサネット・アドレス・テーブル３６、ＩＰハンドラ３８、アドレス翻訳器４０およびユーザ・インタフェース４２を含む。パケットドライバ３０と３２はイーサネット・ハードウェア・インタフェースを制御し、それぞれプライベート・ネットワーク１０と公衆ネットワーク１４と通信する。ＩＰハンドラ３８はメッセージを送受信するためのルータ機能を提供し、ＡＲＰテーブル３４とイーサネット・テーブル３６を保持する。アドレス翻訳器４０は、プラ

イベート・ネットワーク１０からのソース・ポート番号と、公衆ネットワーク側１４上の宛先ポート番号間の翻訳を行う。

ユーザ・インタフェース４２は、処理プラットフォームに付属したキーボードとディスプレイ端末を用いてオペレータがＩＰフィルタ１２にインタフェースすることを可能にする。ファンクションキーは、ＩＰフィルタを計算したり、ログ

ファイルを見たり、コピーしたり、状態を表示したりする。ログファイルはＴＣＰまたはＵＤＰセッションの接続時間、入出力トラフィックの統計、ＩＰフィルタ１２への無効アクセスを含む。ログファイルが大きくなりすぎるのを防ぐために、情報は日付が変わると新しいファイルに登録される。

パケットとＩＰフィルタ１２間のルーティングについては、公衆ネットワーク１４の視点からは公衆インタフェースについて、プライベート・ネットワーク１０の視点からはプライベート・インタフェースについて、以下に記述する。

公衆インタフェースは、ＬＡＮセグメント上でホストとして機能する。公衆インタフェースはパケットを送るために、宛先ＩＰがローカルＬＡＮセグメント上にあるかどうかを確認する。ローカルＬＡＮセグメント上にあった場合、公衆インタフェースはその中のＡＲＰテーブル中でイーサネット・アドレスを探す。ＡＲＰテーブル中にエントリがない場合、公衆インタフェースはパケットを待ち行列に置き、ＡＲＰリクエストを送ってイーサネット・アドレスを取得しなければならない。ＡＲＰテーブル・エントリの標準エージングアウトを実行する必要がある。ＩＰ宛先がＬＡＮセグメント上にない場合、公衆インタフェースはパケットを計算されたデフォルトのルータに送る。デフォルトルータから送られたＩＣＭＰリダイレクトメッセージは無視される。

プライベート・インタフェースは、パケットを１つまたは複数のルータに送り遠隔クライアントのステーションと通信する必要があるため、ルータの機能に影響を与える。大きな遠隔クライアント・ネットワークは、複数のルータマシンにアクセスする場合がある。以前のルート割り当てではルート割り当てエントリがサブネット・アドレスではなくホスト・アドレスになっていたため、ルート割り当てテーブルも大きくなる可能性があった。すなわち、クライアントがルータ１またはルータ２からアクセスできるように設定されているネットワークでは、どのルータもクライアント・ステーションがあるサブネットのルータにはなれないということである。ルート・テーブルをプライベート・ネットワーク上のすべてのルータからＲＩＰを通じて取得するこれまでのルータでは、接続された各遠隔クライアントは大きなホスト・アドレス・テーブルを必要とした。これはルート

を探すために必要な検索時間、巨大なテーブルに必要なメモリ、すべてのルータ間のＬＡＮセグメント上のＲＩＰトラフィックの性能に影響を与える可能性もある。

この環境の中でルーティングを行うために、ＩＰフィルタはイーサネット・テーブルを保持する。プライベート側から公衆側に送られるすべてのパケットに対して翻訳エントリが存在している場合は、イーサネット・インデックスを使って入ってきたパケットのイーサネット・ソース・アドレスと比較する。２つが一致すれば、他の作業は必要ない。一致しなければ、イーサネット・テーブルを検索してソース・イーサネット・アドレスを探し、見つからない場合には新しいイーサネット・テーブル・エントリを追加する。その後、イーサネット・テーブルへのインデックスは、翻訳テーブル・エントリの中に保存される。その後、パケットが公衆側からプライベート側へ翻訳されると、イーサネット・アドレスは翻訳テーブルのインデックスから直接検索することができる。このようにしてパケットはルータへルーティングされ、このルータはパケットをＩＰフィルタに送る。

当業者であれば、本発明の特許請求の範囲から逸れることなく、本発明の実施の形態に対して、さまざまな修正、変更、応用が可能である。したがって、各実施の形態に関し特定の制限がない場合、請求項は上記の実施の形態に制限されることはない。

【図１】

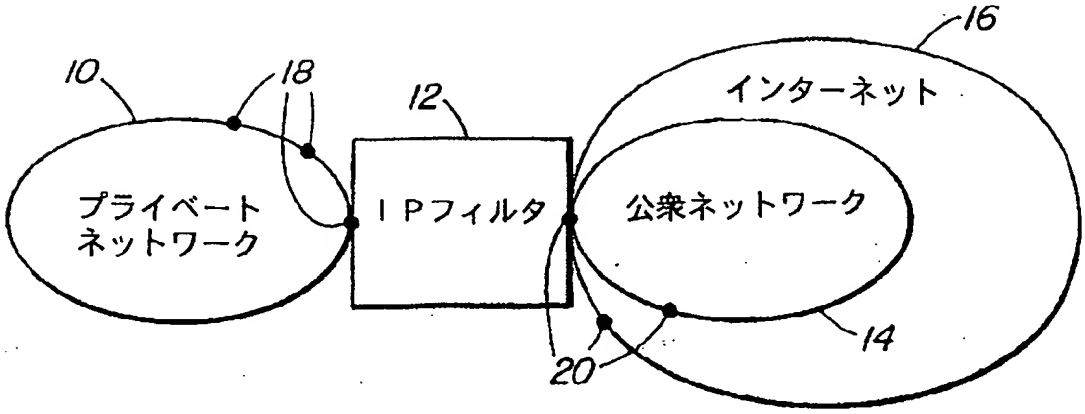


FIG. 1

【図２】

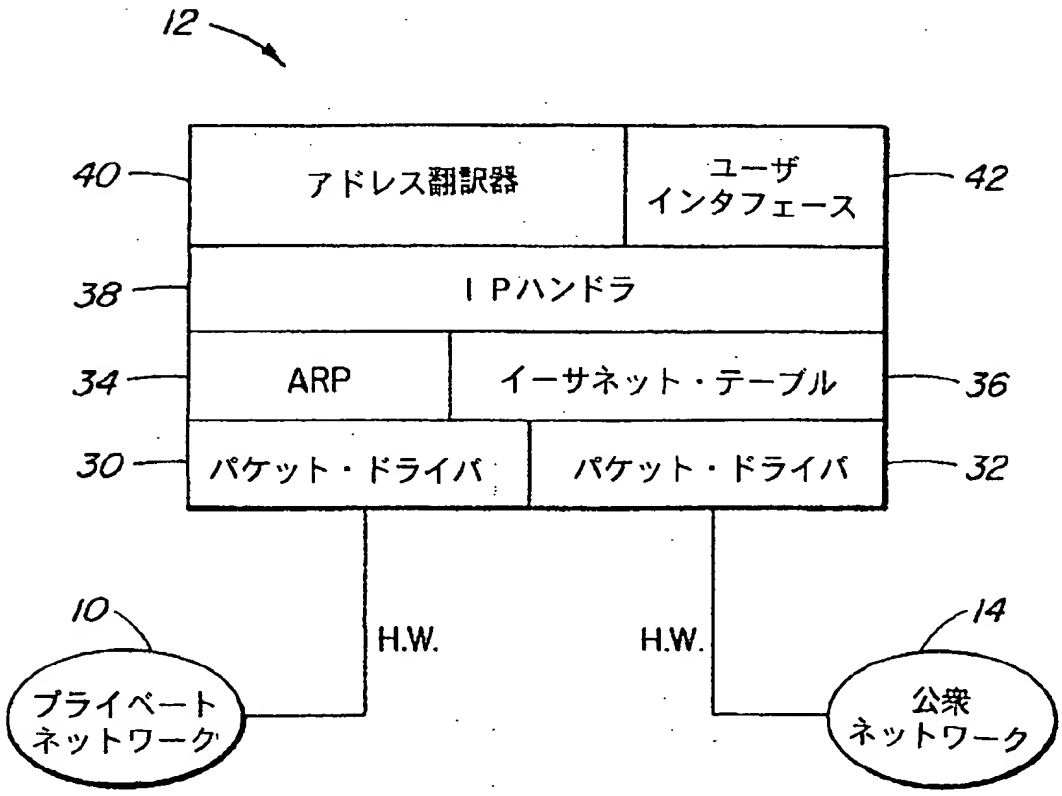


FIG. 2

【手続補正書】特許法第１８４条の８第１項

【提出日】１９９８年４月２０日

【補正内容】

明細書

発明の名称

インターネット・プロトコル・フィルタ

発明の分野

本発明は一般的に、インターネット・ファイアウォールに関する。特に、プライベート・インターネット・プロトコル（ＩＰ）ネットワーク・ドメインを公衆インターネット上の単一ＩＰアドレスにマッピングするインターネット・プロトコル・フィルタに関する。

背景技術

ファイアウォールは、一般的に、プライベート・ネットワークのドメイン内のノードをインターネットのような公衆ネットワーク内のノードに結びつける機能を有するコンピュータサーバとして知られ、特徴づけられる。

エゲバング等は、１９９４年５月、アメリカのインターネットエンジニアリング・タスクフォースの論文「ＩＰネットワーク・アドレス・トランスレータ(ＮＡＴ)」中で、ファイアウォールとして機能するネットワークアドレストランスレータ（ＮＡＴ）を発表した。このＮＡＴは、たとえば、プライベートネットワークのようなＩＰスタブ・ドメイン、およびインターネットのような公衆ネットワークドメインの端に置かれる。ＮＡＴ内のテーブルは一対のローカルＩＰアドレス、すなわち、スタブ・ドメインに対してはローカルで、グローバルには唯一のアドレスであるホストのアドレスから成り立っている。スタブドメイン内のローカルＩＰアドレスはグローバルには唯一ではない。スタブドメイン内のホストが公衆ネットワークドメインを介した通信を必要とする場合、そのローカルＩＰアドレスは、テーブルからグローバルに唯一なＩＰアドレスの１つとペアになっている。ペアになっているグローバルに唯一なＩＰアドレスは、ホストのローカルＩＰアドレスの代わりに公衆ネットワークドメイン内の通信に使われ、これによ

って、一定レベルのセキュリティをホストに提供する。

公知のファイアウォール製品の欠点として、セッションの同時発生または公衆ノードとプライベート・ノード間の相互作用に対して、独自の公衆ＩＰアドレスが必要になることが知られている。このため、公衆ＩＰアドレスを管理するファイアウォールが望まれていた。

発明の概要

本発明の目的は、２つのネットワーク間の通信を結合する新しい改良された装置を提供することにある。

本発明の第１の側面によると、本発明は、第１のデータ通信ネットワークおよび第２のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：宛先情報とソース情報を有するデータパケットを第１のネットワークから受信し、その宛先情報は、第２のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第１のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有し、フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、置き換えられたソース情報を有するデータ・パケットを第２のネットワークに送り、それによってそのパケットは宛先情報に従って対応する第２のネットワーク・ノードにルーティングされるように構成される。

本発明の第２の側面によれば、本発明は、第１のデータ通信ネットワークと第２のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：(ａ)第２のネットワーク内のノードに対応する宛先アドレスと第１のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第１のネットワークから受信し、(ｂ)データ・パケットから抽出されたソース・アドレスを維持し、(ｃ)データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、(ｄ)置き換えられたソース・アドレスを有するデータ・パケットを第２のネットワークに送り、それによってそのパケ

ットは対応の第２のネットワーク・ノードにルーティングされ、(ｅ)置き換えられたソース情報を有するデータ・パケットに応じて、第２のネットワークからの戻りパケットを受信し、(ｆ)戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換え、(ｇ)置き換えられた宛先アドレスを有する戻りパケットを第１のネットワークに送り、それによってそのパケットは対応の第１のネットワーク・ノードにルーティングされるように構成される。

本発明の第３の側面によれば、本発明は、第１のデータ通信ネットワークと第２のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：第２のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有する宛先情報と、第１のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有するソース情報とを有するデータパケットを第１のネットワークから受信する手段と、フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持する手段と、データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換える手段と、置き換えられたソース情報を有するデータ・パケットを第２のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第２のネットワーク・ノードにルーティングする手段とを備えるように構成される。

本発明の第４の側面によると、本発明は、第１のデータ通信ネットワークと第２のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：(ａ) 第２のネットワーク内のノードに対応する宛先アドレスと第１のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第１のネットワークから受信する手段と、(ｂ)データ・パケットから抽出されたソース・アドレスを維持する手段と、(ｃ)データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換える手段と、(ｄ)置き換えられたソース・アドレスを有するデータ・パケットを第２のネットワークに送り、それによってそのパケットを対応の第２のネットワーク・ノードにルーティングする手段と、(ｅ)置き換えられたソース情報を有するデータ・パケットに応じて、第２のネ

ットワークからの戻りパケットを受信する手段と、(ｆ)戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換える手段と、(ｇ)置き換えられた宛先アドレスを有する戻りパケットを第１のネットワークに送り、それによってそのパケットを対応の第１のネットワーク・ノードにルーティングする手段とを備えるように構成される。

本発明で実現されるＩＰフィルタは、公衆ネットワークやインターネット・アクセスをプライベート・ネットワークのノードに供給するために設計された通信デバイスである。ＩＰフィルタは、ネットワーク上でプライベート・ノードを必要とせず、公衆インターネット・アドレスに登録できることを利点とする。ＩＰフィルタはインターネットに単一ＩＰアドレスを与え、複数のＩＰポートを使ってＩＰアドレス管理の問題を解決する。ＩＰフィルタはプライベート側のＩＰセッションをＩＰフィルタの公衆アドレスの単一ポートに割り当てることによってセッションを開始する。これによって最大で64,512(65,536-1,024ポート)の同時セッションが単一ＩＰアドレスでサポートされる。ＩＰフィルタはプライベート・ネットワーク用のソース・ポート番号と、公衆ネットワーク用の宛先ポート番号間で通信を行うための翻訳を行う。

請求の範囲

１．第１のデータ通信ネットワークおよび第２のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：

宛先情報とソース情報を有するデータパケットを第１のネットワークから受信し、その宛先情報は、第２のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第１のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有し、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、

置き換えられたソース情報を有するデータ・パケットを第２のネットワーク

に送り、それによってそのパケットは宛先情報に従って対応する第２のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

2．　請求項1記載の方法において：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第２のネットワークから受信し、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させ、

データ・パケット内で、宛先情報を特定のソース情報と置き換え、

置き換えられた宛先情報を有するデータ・パケットを第１のネットワークに送り、それによってそのパケットが宛先情報に従って対応の第１のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

3．　請求項2記載の方法において：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第２のネットワークから受信されたデータ・パケットを無視することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

4．　請求項3記載の方法において：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアし、ソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

5．　請求項4記載の方法において：

データ・パケットはインターネット・プロトコル（ＩＰ）上で送信制御プロトコル（ＴＣＰ）に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

6. 請求項5記載の方法において：

第1のネットワークからＴＣＰパケットを受信し、そのＴＣＰパケットに対応するエントリがルックアップ・テーブルに見つからず、そのＴＣＰパケットが「これは接続リクエストである」と示した場合、ソース情報をＴＣＰパケットからの宛先情報と共に、ルックアップ・テーブル内の新しいエントリとしてストアすることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

7. 請求項6記載の方法において：

第2のネットワークからＴＣＰパケットを受信し、受信されたＴＣＰパケット内のソース・ポートが、ＴＣＰパケット内の宛先ポートによってインデックスされたルックアップ・テーブルのソース情報エントリ内の宛先ポートと異なり、またＴＣＰパケットが「このパケットが接続リクエストに対する最初の応答である」ことを示した場合には、テーブル・エントリ内の宛先ポートを受信したＴＣＰパケットからのソース・ポートで更新することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

8. 請求項7記載の方法において：

パケット内の送信コードの終端を有するＴＣＰパケットを受信し、受信されたＴＣＰパケットに対応するルックアップ・テーブル内のエントリをゼロにすることことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

9. 請求項4記載の方法において：

データ・パケットはインターネット・プロトコル（ＩＰ）上でデータグラム・プロトコル（ＵＤＰ）に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

10. 請求項9記載の方法において：

第1のネットワークからのＵＤＰデータ・パケットを受信し、ルックアップ・テーブル内の新しいエントリとして、ＵＤＰパケットからのソース情報と宛先情報を経過タイマの期間表示と共に追加することを特徴とする通信ネットワークを

インタフェースするフィルタ・ノードを動作させる方法。

11. 第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：

（a） 第2のネットワーク内のノードに対応する宛先アドレスと第1のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信し、

（b） データ・パケットから抽出されたソース・アドレスを維持し、

（c） データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、

（d） 置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットは対応の第2のネットワーク・ノードにルーティングされ、

（e） 置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信し、

（f） 戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換え、

（g） 置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットは対応の第1のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

12. 請求項11記載の方法において：

戻りパケットを待つ間に第1のネットワークから受信されたータ・パケットをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ（b）から（g）を繰り返すことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

13. 請求項12記載の方法において：

データ・パケットはインターネット制御メッセージ・プロトコル（ICMP）に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースす

るフィルタ・ノードを動作させる方法。

14. 第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：

第2のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有する宛先情報と、第1のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有するソース情報とを有するデータパケットを第1のネットワークから受信する手段と、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持する手段と、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換える手段と、

置き換えられたソース情報を有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第2のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

15. 請求項14記載のフィルタ・ノードにおいて：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第2のネットワークから受信する手段と、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させる手段と、

データ・パケット内で、宛先情報を特定のソース情報と置き換える手段と、

置き換えられた宛先情報を有するデータ・パケットを第1のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第1のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

16. 請求項15記載のフィルタ・ノードにおいて：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第2のネットワークから受信されたデータ・パケットを

無視する手段を備えたことを特徴とするフィルタ・ノード。

17. 請求項16記載のフィルタ・ノードにおいて：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアする手段を備え、そのソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成することを特徴とするフィルタ・ノード。

18. 第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：

（a） 第2のネットワーク内のノードに対応する宛先アドレスと第1のネットフーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信する手段と、

（b） データ・パケットから抽出されたソース・アドレスを維持する手段と、

（c） データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換える手段と、

（d） 置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを対応の第2のネットワーク・ノードにルーティングする手段と、

（e） 置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信する手段と、

（f） 戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換える手段と、

（g） 置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットを対応の第1のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

19. 請求項18記載のフィルタ・ノードにおいて：

戻りパケットを待つ間に第1のネットワークから受信されたデータ・パケッ

トをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ（ｂ）から（ｇ）を繰り返す手段を備えたことを特徴とするフィルタ・ノード。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/CA 97/00269

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RFC1631, May 1994, INTERNET ENGINEERING TASK FORCE, USA, pages 1-10, XP002040992 EGEVANG K AND FRANCIS P: "The IP Network Address Translator (NAT)" see paragraph 2; figures 1,2 see paragraph 3.3 ---	1,11,14, 24,27,31
A	EP 0 465 201 A (DIGITAL EQUIPMENT CORP) 8 January 1992 see column 7, line 30 - column 8, line 27 see column 10, line 45 - column 12, line 22; figure 2 --- -/--	1,11,14, 24,27,31

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 September 1997	14.10.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Dupuis, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/CA 97/00269

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	INTERNET SECURITY HANDBOOK, 1995, MAIDENHEAD, ENGLAND, pages 27-37, XP002040993 STALLINGS W: see page 31; figure 3.2 -----	11,24,31

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inten nal Application No
PCT/CA 97/00269

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0465201 A	08-01-92	US 5309437 A	03-05-94
		CA 2044363 A	30-12-91
		DE 69122439 D	07-11-96
		DE 69122439 T	15-05-97

フロントページの続き

(51) Int. Cl.[6]	識別記号	F I
Ｈ０４Ｌ 29/06		

(72)発明者 コルビン・ウイリアム・ジー.
カナダ国，エル９ティー ４ジェイ６，オンタリオ，ミルトン，チャイルズドライブ 874